Founded 1642

New Hall School

Whole School Acceptable Use Policy for Students

Reviewed by	Senior Leadership & Management Team
Date	August 2018
Authorised by	Board of Governors of New Hall
ISI Code	A8, B17

ACCEPTABLE USE OF TECHNOLOGY POLICY FOR STUDENTS

1 Scope

1.1 This policy is addressed to all students, and parents are encouraged to read it with their child. A copy of the policy is available to parents on request and the School actively promotes the participation of parents to help the School safeguard the welfare of students and promote the safe use of technology.

1.2 The School will take a wide and purposive approach to considering what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets/phablets
- personal music players
- devices with the capability for recording and/or storing still or moving images
- social networking, micro blogging and other interactive web sites
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments such as Firefly
- SMART boards
- other photographic or electronic equipment e.g. GoPro devices.

1.3 This policy applies to the use of technology on School premises.

1.4 This policy also applies to the use of technology off school premises if the use involves students or any member of the School community, or where the culture or reputation of the School are put at risk. Additional rules on the use of technology in boarding houses is provided in the Boarders' Handbook.

1.5 Related policies

1.5.1 Behaviour Policy
1.5.2 Anti-Bullying Policy
1.5.3 Online Safety Policy
1.5.4 Safeguarding and Child Protection Policy

2 Aims

2.1 The aims of this policy are:

2.1.1 to educate and encourage students to make good use of the educational opportunities presented by access to technology;

2.1.2 to safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:

(a) exposure to harmful or inappropriate material (such as pornographic, radicalisation, racist, extremist or offensive materials);

(b) the sharing of personal data, including images, videos and sounds;
(c) inappropriate online contact or conduct; and
(d) cyberbullying and other forms of abuse;

2.1.3 to minimise the risk of harm to the assets and reputation of the School;

2.1.4 to help students take responsibility for their own safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);

2.1.5 to ensure that students use technology safely and securely and are aware of both external and peer to peer risks when using technology;

2.1.6 to prevent the unnecessary criminalisation of students.

3 Safe use of technology

3.1 We want students to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

3.2 The School will support students to develop their skills and make internet access as unrestricted as possible, whilst balancing the safety and welfare of students and the security of our systems. Students are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

3.3 Students may find the following resources helpful in keeping themselves safe online:
http://www.thinkuknow.co.uk/
http://www.childnet.com/
http://www.childline.org.uk/Pages/Home.aspx
http://www.ceop.police.uk

3.4 Please see the School's Online Safety Policy for further information about the School's online safety strategy.

4 Internet and email

4.1 The School provides internet access and an email system to students to support their academic progress and development.

4.2 Students may only access the School's network when given specific permission to do so. All students will receive guidance on the use of the School's internet and email systems. If a student is unsure about whether s/he is doing the right thing, they must seek assistance from a member of staff.

4.3 For the protection of all students, their use of email and of the internet will be monitored by the School. Students should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are always private.

5 School rules

5.1 Students **must** comply with the following rules and principles:

5.1.1 access and security (8.4);

5.1.2 use of internet and email (Appendix 2)

5.1.3 use of mobile electronic device (Appendix 3); and

5.1.4 photographs and images (including "sexting") (Appendix 4).

5.2 The purpose of these rules is to set out the principles, which students must bear in mind at all times, and also the rules which students must follow to use technology safely and securely.

5.3 These principles and rules apply to all use of technology.

6 Procedures

6.1 Students are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a student is aware of misuse by other students s/he should report it to a teacher as soon as possible.

6.2 Any misuse of technology by students will be dealt with under the School's Behaviour Policy.

6.3 Students must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If a student thinks that s/he might have been bullied or that another person is being bullied, s/he should talk to a teacher about it as soon as possible. See also the School's Anti-Bullying Policy.

6.4 In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's Safeguarding & Child Protection Policy. If a student is worried about something that s/he has seen on the internet, or on any electronic device, including on another person's electronic device, s/he must tell a teacher about it as soon as possible.

6.5 In a case where the student is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

6.6 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the IT Manager who will record the matter centrally in the Technology Incidents Log.

7 Sanctions

7.1 Where a student breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Governors have authorised the Principal to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Behaviour Policy including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures, withdrawal of the right to access the School's internet and email facilities and/or detention. Any action taken will depend on the seriousness of the offence.

7.2 Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy and the School's Behaviour Policy and Searching a Student and/or their Possessions Policy for the School's policy on the searching and confiscation of electronic devices.

7.3 The School reserves the right to charge a student or his / her parents for any costs incurred to the School as a result of a breach of this policy.

8 Monitoring and review

8.1 All serious technology safety incidents will be logged centrally in the Technology Incident Log by the Chair of the Safeguarding Committee and the IT Manager.

8.2 The Head of ICT & Computing, IT Manager and the Chair of the Safeguarding Committee have responsibility for the implementation and review of this policy:

8.2.1 The IT Manager is responsible for the effective operation of the School's network. S/he monitors the use of technology as set out in this policy and maintains the appropriate logs and will review the policy on a regular basis to ensure that it remains up to date with technological changes.

8.2.2 The Chair of the Safeguarding Committee will consider the record of technology safety incidents and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and safety practices within the School are adequate.

8.3 Consideration of the efficiency of the School's e-safety procedures and the education of students about keeping safe online will be included in the annual review of safeguarding for Governors.

8.4 APPENDIX 1

Access and Security

1. Access to the internet from the School's devices and network must be for educational purposes only. You must not use the School's facilities or network for personal, social or non-educational use outside the permitted times specified by the School / without the express, prior consent of a member of staff.
2. You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.
3. No laptop or other mobile electronic device may be connected to the School network without the consent in writing of the IT Support Manager and the Head of ICT & Computing, who in turn will check that appropriate anti-virus software is installed on the device.
4. The use of cellular data (e.g. GPRS, 3G, 4G, etc.) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.
5. Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.
6. You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher or contact the ICT support.
7. You must not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.
8. The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or IT Manager.
9. The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of students. You must not try to bypass this filter.
10. Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to IT Manager before opening the attachment or downloading the material.
11. You must not disable or uninstall any anti-virus software on the School's computers.
12. The use of location services represents a risk to the personal safety of students and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.
13. You are responsible for ensuring that all requested operating system updates are performed on your school tablet. These will help provide important security patches, which will help to keep you and your data safe online.

14. It is an expectation that school tablets have Bluetooth turned on at all times as this will enable staff to monitor your safe use of online resources and applications.

15. You must not attempt to add applications to the any device without the express consent of the IT Manager and the Head of ICT & Computing. Requests for educational applications are welcome using the online form on the school's Firefly VLE.

16. Methods for overcoming limitations placed on a school device such as 'jailbreaking' are treated with the upmost seriousness.

APPENDIX 2

1 Use of internet and email

1.1 The School does endeavours to provide continuous internet access. Email and website addresses at the School may change from time to time.

2 Use of the internet

2.1 You must use the School's computer system for educational purposes only and are not permitted to access interactive or networking web sites outside the permitted times specified by the School / without the express prior consent of a member of staff.

2.2 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

2.3 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the IT Manager.

2.4 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

2.5 You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

2.6 You must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

2.7 You must not bring the School into disrepute through your use of the internet.

3 Use of email

3.1 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail through the School's network outside the permitted times specified by the School / without the express, prior consent of a member of staff. This will be unnecessary as you are provided with you own personal email account for School purposes.

3.2 Your School email accounts can be accessed from home by OneDrive. The School will not forward emails received during the School holidays.

3.3 You must use your School email accounts for any email communication with staff. Communication either from a personal, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

3.4 Trivial messages and jokes should not be sent or forwarded through the School's email system. Not only could these cause distress to recipients (if considered to be inappropriate), but could also cause the School's network to suffer delays and / or damage.

3.5 All correspondence from your School email account will contain the School's disclaimer.

3.6 You must not read anyone else's emails without their consent.

APPENDIX 3

Use of mobile devices

1. "Mobile electronic device" includes but is not limited to mobile phones, smartphones, smart watches, tablets, laptops and MP3/MP4 players.

2. All mobile electronic devices brought onto School premises are not permitted to be registered on the school's Wi-Fi network unless in the Sixth Form.

3. Students in Years 7-11 are not permitted to use their mobile phones or smartphones (including the use of smart watches) during the normal academic school day (this includes break and lunchtimes). All personal electronic devices must be stored in the lockers provided, secured with a padlock. Mobile phones or smartphones should be on silent mode. Please be aware that the school insurance does not cover the loss of mobile phones.

4. Students in Years 7-11 are permitted to have their mobile phones or smartphones out and visible to the teacher in after school study, in order only to receive messages regarding pickup from school.

5. If a student in Years 7-11 is seen using a mobile or smart phone during the normal academic school day then it will be confiscated for a 24 hour period and students will receive a Yellow Card. If, however, the student needs the device for safe travel home then this can be collected at the end of the school day from student reception but must be returned to student reception no later than 8.10am the following school day.

6. For Sixth Form students, mobile phones are permitted only in the Sixth Form area.

7. All devices are brought into school at the student's own risk. All devices should require a pass code or password to be unlocked and this should never be divulged to any other student.

8. The use of cellular data (e.g. GPRS, 3G, 4G, etc.) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

9. The use of mobile phones during the School day will not be necessary. In emergencies, you may request to use the School telephone. Should your parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.

10. You must not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the Principal in writing.

11. You must not communicate with staff using a mobile phone (or other mobile electronic device), except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

12. Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-Bullying Policy and Behaviour Policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's Safeguarding and Child Protection Policy and Procedures).

13. Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see Appendix of the School's Behaviour Policy on the searching of electronic devices. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Head.

14. The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

APPENDIX 4

Photographs and images

1. Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2. No photograph should be taken of any other student without their express permission.

3. You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.

4. You must allow staff access to images stored on mobile phones, cameras or devices and must delete images if requested to do so.

5. The posting of images which in the reasonable opinion of the Principal is considered to be offensive or which brings the school into disrepute on any form of social media or websites such as YouTube etc. is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

6. Sexting:

6.1 'Sexting' means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet.

6.2 Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

6.3 Sexting may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.

6.4 Remember that once a photograph or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

6.5 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

6.6 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding and Child Protection Policy).

6.7 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.